UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,932	11/26/2001	Akiko Miyagawa	2565-0238P	9870

2292 7590 02/06/2006

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 02/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/991,932	MIYAGAWA ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-13 and 17* is/are rejected.

7)☐ Claim(s) *6 and 14-16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/10/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicants' response received on November 10, 2005.

2. Amendments of claims 2, 4 and 10 are acknowledged.

3. Addition of new claims 13-17 are acknowledged.

4. Applicants' arguments have been fully considered but they are not persuasive.

5. Applicants argue (p. 10, l. 1-5) that "However, Rothermel fails to disclose, at least, an illegal access data handling device, being placed outside a given internal communications network," as recited in claim 1" and "a method for handling illegal access data outside a given internal communication network,...receiving illegal access data transmitted from a data communication device placed outside the internal communications network,' as recited in claim 9."

Rothermel discloses a network security device (NSD) located between an internal network and an external network (see Fig. 1, 130, 135 and 190; Fig. 2, 130, 20-230) that monitors information traffics between external and internal devices (see col. 14, l. 52-54) in order to allow authorized user to have access to the internal network (see col. 5, l. 55-67; col. 6, l. 15-19). Rothermel further discloses that external users or customers must provide specific information to an NSD such as password, a key, etc. in order to be allowed to contact or have access to an internal device (see col. 5, l. 61-67; col. 11, l. 24-61). This arrangement constitutes a method equivalent the method of claim 9.

6. In light of the above submission the previous rejection of the original claims and the rejection of the new claims are presented as follows.

Claim Rejections - 35 USC § 112

The following is a quotation of the **first paragraph** of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1 and 2 are rejected under 35 U.S.C. 112, first paragraph, because these claims while reciting the location and purpose of an illegal access data handling apparatus, but fail to specify the scope of an apparatus what is composed of. Moreover, it is not clear whether an apparatus or a method steps being claimed.

The following is a quotation of the **second paragraph** of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 and 2 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1 and 2 provide for the location and purpose of an illegal access data handling apparatus, but do not set forth a method steps or an apparatus claims.

Claim 13 recites the limitation "the network device" in line 9. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-3 and 9-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Rothermel et al (6,678,827 B1; hereinafter Rothermel).

Claim 1

Rothermel discloses:

An illegal access data handling apparatus, being placed outside a given internal communication network (see col. 1, lines 22-36, where unauthorized external access corresponds to the recited illegal access data; col. 6, lines 7-20, where the Network Security Device Management and the supervisor devices are functionally equivalent to

the recited illegal access data handling apparatus; col. 14, lines 50-59), for receiving illegal access data transmitted from a data communication device placed outside the internal communication network for a purpose of illegally accessing the internal communication network (see col. 6, lines 7-20; col. 9, lines 14-27, where an NSD transmits security information about an event of interest corresponding to the recited illegal access data to a supervisor device), and for taking countermeasures against the illegal access data received (see col. 15, lines 30-57).

Claim 2

Rothermel discloses:

The illegal access data handling apparatus of claim 1, wherein the illegal access data handling apparatus is connected to an illegal access data detection device for relaying a data communication between a data communication device placed within the internal communication network and a data communication device placed outside the internal communication network (see col. 4, lines 30-48; col. 6, lines 7-20, where the Network Security Device Management and the supervisor devices are functionally equivalent to the recited illegal access data handling apparatus and the Network Security Device that is placed between external devices and the internal devices corresponds to the recited illegal access data detection device), and for detecting the illegal access data, and wherein the illegal access data handling apparatus receives the illegal access data from the illegal access data detection device (see col. 15, lines 3-15;

col. 16, lines 7-55, where the NSD detects unauthorized packets and transmits information related to this event to a supervisor device).

Claim 3

Rothermel discloses:

The illegal access data handling apparatus of claim 2, comprising:

a data reception section for receiving the illegal access data from the illegal access data detection device (see col. 16, lines15-20);

a data analysis section for analyzing the illegal access data received by the data reception section (see col. 3, lines 45-57; col. 4, lines 43-48);

a response data generation section for generating response data to the illegal access data based upon an analysis result from the data analysis section (see col. 4, line 49-col. 5, line 13, where the templates corresponds to the recited response data); and

a data transmission section for transmitting the response data generated by the response data generation section to the illegal access data detection device (see col. 4, lines 65-col. 5, line 3).

Claim 9

Rothermel discloses:

A method for handling illegal access data outside a given internal communication network, the method comprising (see Fig. 1):

receiving illegal access data transmitted from a data communication device placed outside the internal communication network for a purpose of illegally accessing the internal communication network (see col. 6, lines 7-20; col. 9, lines 14-27, where a NSD transmits security information about an event of interest corresponding to the recited illegal access data to a supervisor device); and

taking countermeasures against the illegal access data received (see col. 15, lines 30-57).

Claim 10

Rothermel discloses:

The method of claim 9, comprising:

communicating with an illegal access data detection device for relaying a data communication between a data communication device placed within the internal communication network and a data communication device placed outside the internal communication network, and for detecting the illegal access data (see col. 4, lines 30-48; col. 6, lines 7-20, where the Network Security Device Management and the supervisor devices are functionally equivalent to the recited illegal access data handling apparatus and the Network Security Device that is placed between external devices and the internal devices corresponds to the recited illegal access data detection device); and receiving the illegal access data from the illegal access data detection device (see col. 15, lines 3-15; col. 16, lines 7-55, where the NSD detects unauthorized packets and transmits information related to this event to a supervisor device).

Claim 11

Rothermel discloses:

The method of claim 10, comprising:

receiving the illegal access data from the illegal access data detection device (see col. 16, lines15-20);

analyzing the illegal access data received by the receiving (see col. 3, lines 45-57; col. 4, lines 43-48);

generating response data to the illegal access data based upon an analysis result from the analyzing (see col. 4, line 49-col. 5, line 13, where the templates corresponds to the recited response data); and

transmitting the response data generated by the generating to the illegal access data detection device (see col. 4, lines 65-col. 5, line 3).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 7, 8, 13 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothermel et al (6,678,827 B1; hereinafter Rothermel) in view of Reshef et al (6,321,337 B1; hereinafter Reshef).

Claim 4

Rothermel discloses:

The illegal access data handling apparatus of claim 3, wherein the data reception section receives an illegal access data from the illegal access data detection device (see col. 5, lines 55-61; col. 16, lines 15-20), and wherein the data transmission section transmits the response data to the illegal access data detection device (see col. 5, lines 55-61; col. 16, lines 15-20; col. 17, lines 23-43)

Rothermel does not expressly discloses that the illegal access data handling apparatus includes a capsulation section for decapsulating the encapsulated illegal access data received by the data reception section to extract the illegal access data, and encapsulates the response data.

Reshef, however, discloses a system for protecting an internal network from attacks originated from entities located in an external network (see col. 3, lines 45-67). Reshef further discloses a capsulation mechanism deployed in security components of a gateway to encapsulate and decapsulate the data transmitted between them. Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to implement a capsulation mechanism as taught in Reshef in the system of Rothermel, because it would reinforce the communication between a NSD (a detecting device) and a supervisor device (a security managing device) against exploitation and against bugs affecting the operation (see Reshef, col. 2, lines 15-30).

Claim 7

Rothermel discloses:

The illegal access data handling apparatus of claim 4, wherein the data reception section receives the illegal access data having authentication information attached to be used for data authentication from the illegal access data detection device, and wherein the capsulation section performs the data authentication for the illegal access data by using the authentication information (see col. 6, lines 1-6; col. 11, lines 34-45).

Claim 8

Rothermel discloses:

The illegal access data handling apparatus of claim 7, wherein the capsulation section attaches the authentication information to be used for the data authentication for the response data to the response data, and wherein the data transmission section transmits the response data having the authentication information attached by the capsulation section to the illegal access data detection device (see col. 5, line 52-col. 6, line 6; col. 11, lines 34-45, where the communication between the NSDs and supervisor devices are encrypted and authenticated for the purpose of security and thus, the information transmitted between these devices must have required data to perform authentication process).

Claims 13 and 17

Rothermel discloses:

receiving an unauthorized access packet at a data center placed outside the internal network, and wherein the unauthorized access packet is redirected from a target server residing within the internal network (see col. 6, lines 7-20; col. 9, lines 14-27; col. 16, lines15-20);

analyzing the received packet to formulate a response packet (see col. 3, lines 45-57; col. 4, lines 43-48);

sending the response packet to the network device, wherein the network device is within the internal network (see col. 4, lines 65-col. 5, line 3, where the templates corresponds to the recited response data).

Rothermel does not expressly discloses that the illegal access data handling apparatus includes a capsulation section for decapsulating the encapsulated illegal access data received by the data reception section to extract the illegal access data, and encapsulates the response data.

Reshef, however, discloses a system for protecting an internal network from attacks originated from entities located in an external network (see col. 3, lines 45-67). Reshef further discloses a capsulation mechanism deployed in security components of a gateway to encapsulate and decapsulate the data transmitted between them.

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to implement a capsulation mechanism as taught in Reshef in the system of Rothermel, because it would reinforce the communication between a NSD (a detecting device) and a supervisor device (a security managing device) against exploitation and against bugs affecting the operation (see Reshef, col. 2, lines 15-30).

Claims 5 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothermel et al (6,678,827 B1; hereinafter Rothermel) in view of Moran (6,826,697 B1; hereinafter Moran).

Regarding claims 5 and 12, Rothermel does not discloses a decoy scheme to respond to an illegal access attempt by an unauthorized user (e.g. a hacker) with a response to have similar content as a true response. Moran teaches the use of a deception server containing false data to be used by suspected users (col. 2, lines 1-5). Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to implement a decoy computer system as taught in Moran in the system of Rothermel, in order to defeat the attackers attempting to access a computer system (see Moran, col. 1, lines 57-62).

Allowable Subject Matter

Claims 6 and 14-16 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132 A. N.

January 26, 2006

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100